

(3) Vouchers redeemed while the voucher system was temporarily out of operation must be validated as expeditiously as possible upon restored operation of the voucher system.

(4) Paid vouchers must be maintained in the cashier's accountability for reconciliation purposes.

(5) Unredeemed vouchers can only be voided in the voucher system by supervisory employees. The accounting department will maintain the voided voucher, if available.

(i) *Cage and vault access.* Controls must be established and procedures implemented to:

(1) Restrict physical access to the cage to cage agents, designated staff, and other authorized persons; and

(2) Limit transportation of extraneous items such as personal belongings, tool boxes, beverage containers, etc., into and out of the cage.

(j) *Variances.* The operation must establish, as approved by the TGRA, the threshold level at which a variance must be reviewed to determine the cause. Any such review must be documented.

§ 543.19 [Reserved]

§ 543.20 What are the minimum internal control standards for information technology and information technology data?

(a) *Supervision.* (1) Controls must identify the supervisory agent in the department or area responsible for ensuring that the department or area is operating in accordance with established policies and procedures.

(2) The supervisory agent must be independent of the operation of Class II games.

(3) Controls must ensure that duties are adequately segregated and monitored to detect procedural errors and to prevent the concealment of fraud.

(4) Information technology agents having access to Class II gaming systems may not have signatory authority over financial instruments and payout forms and must be independent of and restricted from access to:

- (i) Financial instruments;
- (ii) Accounting, audit, and ledger entries; and
- (iii) Payout forms.

(b) As used in this section only, a system is any computerized system that is integral to the gaming environment. This includes, but is not limited to, the server and peripherals for Class II gaming system, accounting, surveillance, essential phone system, and door access and warning systems.

(c) Class II gaming systems' logical and physical controls. Controls must be established and procedures implemented to ensure adequate:

(1) Control of physical and logical access to the information technology environment, including accounting, voucher, cashless and player tracking systems, among others used in conjunction with Class II gaming;

(2) Physical and logical protection of storage media and its contents, including recovery procedures;

(3) Access credential control methods;

(4) Record keeping and audit processes; and

(5) Departmental independence, including, but not limited to, means to restrict agents that have access to information technology from having access to financial instruments.

(d) *Physical security.* (1) The information technology environment and infrastructure must be maintained in a secured physical location such that access is restricted to authorized agents only.

(2) Access devices to the systems' secured physical location, such as keys, cards, or fobs, must be controlled by an independent agent.

(3) Access to the systems' secured physical location must be restricted to agents in accordance with established policies and procedures, which must include maintaining and updating a record of agents granted access privileges.

(4) Network Communication Equipment must be physically secured from unauthorized access.

(e) *Logical security.* (1) Controls must be established and procedures implemented to protect all systems and to ensure that access to the following is restricted and secured:

- (i) Systems' software and application programs;
- (ii) Data associated with Class II gaming; and